GROWTH OF SELMER GROUPS OVER FUNCTION FIELDS

AFTAB PANDE

Abstract. We study the rank of the p-Selmer group $Sel_p(A/k)$ of an abelian variety A/k, where k is a function field. If K/k is a quadratic extension and F/k is a dihedral extension and the $\mathbb{Z}_p$-corank of $Sel_p(A/K)$ is odd, we show that the $\mathbb{Z}_p$-corank of $Sel_p(A/F) \geq [F : K]$. The result generalizes the theory of local constants developed by Mazur-Rubin for elliptic curves over number fields.

1. Introduction

If E is an elliptic curve over $\mathbb{Q}$, then the Birch and Swinnerton-Dyer conjecture predicts that the order of vanishing of the associated L-function is equal to the rank of E i.e. $ord_{s=1}L(E/\mathbb{Q}, s) = rkE/\mathbb{Q}$. One of the consequences of this famous conjecture is the parity conjecture (recently proved by the Dokchitser brothers [DD1], [DD2]) which states that $(-1)^{rkE/\mathbb{Q}} = w(E/\mathbb{Q})$, where $w(E/\mathbb{Q})$ is the root number of the associated L-function.

However, determining the rank of a given elliptic curve is a hard problem. If we assume the Tate-Shafarevich conjecture about the finiteness of Ш(E/K), then the $\mathbb{Z}_p$-corank of the corresponding p-Selmer group $Sel_p(E/K)$ has essentially the same rank as $E(K)$.

Let A an abelian variety over k, a function field of characteristic $q > 0$ and assume that A has a polarization of degree prime to p, where $p \neq q$. Let K/k be a quadratic extension with F/K an abelian extension, dihedral over k. We wish to study the $\mathbb{Z}_p$-corank of the p-Selmer group $Sel_p(A/F)$. In [P], Pacheco obtained upper bounds for the $\mathbb{Z}_p$-corank of $Sel_p(A/K)$ and, as a consequence, got an upper bound for the $\mathbb{Z}$-rank of the Lang-Neron group. In

[MR] a lower bound was obtained for the $\mathbb{Z}_p$-corank of the corresponding p-Selmer group $Sel_p(E/F)$ and we follow their approach. We assume that the $\mathbb{Z}_p$-corank of $Sel_p(A/K)$ is odd and show that the $\mathbb{Z}_p$-corank of $Sel_p(A/F) \geq [F:K]$.

One of the key ideas in the proof is to decompose $Sel_p(A/F) \cong \oplus_L Sel_p(A_L/K)$, where A_L is an abelian variety and L runs through the cyclic extensions of K contained in F. We will then show that

$$corank_{\mathbb{Z}_p} Sel_p(A_L/K) \equiv corank_{\mathbb{Z}_p} Sel_p(A/K) (\mod 2).$$

As $corank_{\mathbb{Z}_p} Sel_p(A/K)$ was assumed to be odd, it follows that the $\mathbb{Z}_p$-corank of $Sel_p(A/F) \geq [F:K]$.

To show that $corank_{\mathbb{Z}_p} Sel_p(A_L/K) \equiv corank_{\mathbb{Z}_p} Sel_p(A/K) (\mod 2)$, we will first show that

$$corank_{\mathbb{Z}_p} Sel_p(A_L/K) - corank_{\mathbb{Z}_p} Sel_p(A/K) \equiv \textstyle\sum_{v\in S} \delta_v (\mod 2),$$

where S is a finite set of primes v of K and the δ_v depend only on A and the local extensions of K_v. Finally, we will show that for primes v of good reduction the local invariants $\delta_v = 0$, completing the argument.

This article is based almost entirely on the paper of [MR]. We have merely adapted their methods for elliptic curves over number fields to abelian varieties over function fields.

2. Duality results

Let C be a smooth, geometrically connected curve over a finite field $\mathbb{F}$ of characteristic $q > 0$ and let $k = \mathbb{F}^s(C)$ be its function field, where $\mathbb{F}^s$ is the separable closure of $\mathbb{F}$. Let A/k be a non-constant abelian variety of dimension d defined over k with a polarization prime to p. A model for A/K consists of a smooth, geometrically connected projective variety $\mathcal{A}$ defined over k and a proper flat morphism $\phi : \mathcal{A} \to C$ also defined over k whose generic fibre is A/k. Let U be the maximal open dense subscheme of C over which $\mathcal{A}$ is smooth and $\mathcal{A}_U = \phi^{-1}(U)$. The morphism ϕ induces an abelian

scheme $\phi_U : \mathcal{A}_U \to U$, which still has A/K as its generic fibre. Let Q be the set $C(\mathbb{F}^s) \setminus U(\mathbb{F}^s)$.

Let $C_s := C \times_{Spec(k)} Spec(k^s)$, $U_s := U \times_{Spec(k)} Spec(k^s)$, η_s the geometric generic point of U_s and let $\pi(U_s, \eta_s)$ be the algebraic fundamental group of U_s with respect to η_s. Let k^{ur} be the maximal Galois subextension of k^s/k that is unramified over U, so $\pi(U_s, \eta_s) \cong Gal(k^{ur}/k)$. Let $\pi^t(U_s, \eta_s)$ be the tame algebraic fundamental group, so $\pi^t(U_s, \eta_s) \cong Gal(k^{tr}/k)$, where k^{tr} is the maximal Galois subextension of k^s/k, which is unramfied over U_s and at most tamely ramified over $C_s \setminus U_s$. Let $\pi_v(U_s, \eta_s)$ be the local fundamental group, $\pi_v^t(U_s, \eta_s)$ the local tame fundamental group, $G_v := Gal(k_v^s/k_v)$ and $R_v := Gal(k_v^s/k_{tr})$ (wild inertia).

Following [M] and [E], we can define a Selmer group using the language of sheaves and the fundamental group as follows.

Definition. Let $j : \eta_s \hookrightarrow C_s$ be the inclusion of the generic point, and let $\mathcal{W}$ be a discrete p-primary torsion sheaf on the etale site of η_s. Let $\mathcal{M} = j_*\mathcal{W}$ and define the Selmer group $S(C, \mathcal{W})$ as $H^1(C_s, \mathcal{M})$

Definition. Let W be a constant p-primary torsion sheaf. A Selmer structure $\mathcal{F}$ on W is a collection of subspaces $H^1_{\mathcal{F}}(\pi_v(U_s, \eta_s), W) \subset H^1(\pi_v(U_s, \eta_s), W)$ for every place v of k such that $H^1_{\mathcal{F}}(\pi_v(U_s, \eta_s), W) = H^1((G_v/I_v), W^{I_v})$ for all but finitely many v, where I_v is the inertia subgroup of G_v.

If $\mathcal{F}$ and $\mathcal{G}$ are two Selmer structures we define $\mathcal{F} + \mathcal{G}$ and $\mathcal{F} \cap \mathcal{G}$ by:

$$H^1_{\mathcal{F}+\mathcal{G}}(\pi_v(U_s, \eta_s), W) := H^1_{\mathcal{F}}(\pi_v(U_s, \eta_s), W) + H^1_{\mathcal{G}}(\pi_v(U_s, \eta_s), W),$$
$$H^1_{\mathcal{F}\cap\mathcal{G}}(\pi_v(U_s, \eta_s), W) := H^1_{\mathcal{F}}(\pi_v(U_s, \eta_s), W) \cap H^1_{\mathcal{G}}(\pi_v(U_s, \eta_s), W).$$

Now we can reformulate the definition of the Selmer group in terms of Selmer structures.

Definition. The Selmer group relative to a Selmer structure $\mathcal{F}$ can be defined as

$$H^1_{\mathcal{F}}(\pi(U_s, \eta_s), W) := Ker\{H^1(\pi(U_s, \eta_s), W) \to \prod_v H^1(\pi_v(U_s, \eta_s), W)/H^1_{\mathcal{F}}(\pi_v(U_s, \eta_s), W)\}$$

Theorem 2.1. *(Tate Local Duality) Let μ be the group of roots of unity, W an unramified G_v-module, $W^D = Hom(W, \mu)$ and assume that $\#tor(W)$ is prime to char k. If I_v is the inertia subgroup of G_v, then for $0 \leq i \leq 2$ the groups $H^i(G_v/I_v, W)$ and $H^{2-i}(G_v/I_v, W^D)$ annihilate each other in the pairing*

$$H^i(G_v, W) \times H^{2-i}(G_v, W^D) \to H^2(G_v, \overline{k_v}^*) \to \mathbb{Q}/\mathbb{Z}.$$

They are mutually orthogonal for $i = 1$.

We say that a Selmer structure for W is self dual if for every v, $H^1_{\mathcal{F}}(\pi_v(U_s, \eta_s), W)$ is its own orthogonal complement under the Tate pairing defined above.

Now, let $W = A[p]$, the p-torsion points of the abelian variety A. The first Selmer structure $H^1_{\mathcal{E}}(\pi_v(U_s, \eta_s), A[p])$ is defined as the image in $H^1(\pi_v(U_s, \eta_s), A[p])$ of the Kummer injection

$$A(k_v)/pA(k_v) \hookrightarrow H^1(\pi_v(U_s, \eta_s), A[p])$$

for every v.

By Lemma 2.1 of [P], we know that $H^1_{\mathcal{E}}(\pi_v(U_s, \eta_s), A[p]) = H^1(G_v/I_v, A[p])$ for all $v \in U_s$. The Selmer group $H^1_{\mathcal{E}}(\pi(U_s, \eta_s), A[p])$ as defined by the Selmer structure $\mathcal{E}$ is the usual p-Selmer group $Sel_p(A/K)$. By Tate local duality, we know that this Selmer structure is self-dual.

If $q > 2d + 1$ then by Lemma 2.4 of [P] we know that for $v \in C_s \setminus U_s$ the ramification group R_v acts trivially on $A[p^n]$. Thus, the natural descent map

$$\delta_{p^n} : A(k)/p^n A(k) \hookrightarrow H^1(\pi_1(U_s, \eta_s), A[p^n])$$

factors through the tame fundamental group

$$\delta_{p^n} : A(k)/p^n A(k) \hookrightarrow H^1(\pi^t(U_s, \eta_s), A[p^n])$$

Hence, we can modify the Selmer group definition using the tame fundamental group.

Definition. The Selmer group relative to the Selmer structure $\mathcal{E}$ can be defined as

$$H^1_{\mathcal{E}}(\pi(U_s,\eta_s),W) := Ker\{H^1(\pi^t(U_s,\eta_s),W) \to \prod_v H^1(\pi^t_v(U_s,\eta_s),W)/H^1_{\mathcal{E}}(\pi^t_v(U_s,\eta_s),W)\}$$

The cup product pairing is used to prove the duality theorem. If $f \in H^i(G_v,W)$ and $g \in H^{2-i}(G_v,W^D)$, then the cup product $f \cup g \in H^2(G_v,\overline{k_v}^*)$ is defined as $(f \cup g)(\sigma_1,\sigma_2) = f(\sigma_1) \otimes \sigma_1 g(\sigma_2)$. When f,g are unramified we see that $f \cup g \in H^2(G_v/I_v,\overline{k_v}^*)$, but as the cohomological dimension of $G_v/I_v = \hat{\mathbb{Z}}$ is 1, we see that f,g are the exact annihilators of each other under the cup product pairing. We can modify this pairing for the tame fundamental group on:

$$<,>_v: H^i(\pi^t_v(U_s,\eta_s),W) \times H^{2-i}(\pi^t_v(U_s,\eta_s),W^D) \to H^2(\pi^t_v(U_s,\eta_s),\overline{k_v}^*) \to \mathbb{Q}/\mathbb{Z}.$$

As $\pi^t_v(U_s,\eta_s) = Gal(k_v^{tr}/k_v) = \widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}'$, whose cohomological dimension is never 1, we see that the cup product pairing makes sense. If f,g are unramified we see that they are the exact annihilators of each other, following the argument above. Hence, the notion of self-dual Selmer structures works for tame fundamental groups as well.

The following result (essentially Prop 1.3 of [MR]) about self-dual Selmer structures is crucial in the rest of the paper. It allows us to compute the difference in the $\mathbb{F}_p$-dimensions of the two Selmer groups locally. Later, we will corelate the $\mathbb{F}_p$-dimension to the $\mathbb{Z}_p$-corank.

Theorem 2.2. *Suppose that $\mathcal{F},\mathcal{G}$ are self-dual Selmer structures on W, and S is a finite set of places of K such that $H^1_{\mathcal{F}}(\pi^t_v(U_s,\eta_s),W) = H^1_{\mathcal{G}}(\pi^t_v(U_s,\eta_s),W)$ if $v \notin S$ then:*

$$dim_{\mathbb{F}_p} H^1_{\mathcal{F}}(\pi^t(U_s,\eta_s),W) - dim_{\mathbb{F}_p} H^1_{\mathcal{G}}(\pi^t(U_s,\eta_s),W)$$
$$\equiv \sum_{v\in S} dim_{\mathbb{F}_p}(H^1_{\mathcal{F}}(\pi^t_v(U_s,\eta_s),W)/H^1_{\mathcal{F}\cap\mathcal{G}}(\pi^t_v(U_s,\eta_s),W)) \pmod 2.$$

Proof. Let $B = \oplus_{v\in S} H^1_{\mathcal{F}+\mathcal{G}}(\pi^t_v(U_s,\eta_s),W)/H^1_{\mathcal{F}\cap\mathcal{G}}(\pi^t_v(U_s,\eta_s),W)$ and let C be the image of the localisation map from $H^1_{\mathcal{F}+\mathcal{G}}(\pi^t(U_s,\eta_s),W) \to B$. So,

$$C \cong H^1_{\mathcal{F}+\mathcal{G}}(\pi^t(U_s,\eta_s),W)/H^1_{\mathcal{F}\cap\mathcal{G}}(\pi^t(U_s,\eta_s),W).$$

Let $C_{\mathcal{F}}$ (resp. C_G) be the image of $\oplus_{v\in S}H^1_{\mathcal{F}}(\pi^t_v(U_s,\eta_s),W)$ (resp. $\oplus_{v\in S}H^1_{\mathcal{G}}(\pi^t_v(U_s,\eta_s),W)$) in B, so that

$$C_{\mathcal{F}} = \oplus_{v\in S}H^1_{\mathcal{F}}(\pi^t_v(U_s,\eta_s),W)/H^1_{\mathcal{F}\cap\mathcal{G}}(\pi^t_v(U_s,\eta_s),W).$$

Using the Tate Pairing $<,>_v$ above, we can define another pairing

$$<,>_B\colon B\times B\to\mathbb{F}_p$$

If $(\beta,\beta')\in B\times B$, where $\beta=(f_v+g_v)_{v\in S}$, $\beta'=(f'_v+g'_v)_{v\in S}$, such that $f_v\in H^1_{\mathcal{F}}(\pi^t_v(U_s,\eta_s),W)$ but $f_v\notin H^1_{\mathcal{G}}(\pi^t_v(U_s,\eta_s),W)$ and $g_v\in H^1_{\mathcal{G}}(\pi^t_v(U_s,\eta_s),W)$ but $g_v\notin H^1_F(\pi^t_v(U_s,\eta_s),W)$ for all $v\in S$. Then $<\beta,\beta'>_B:=\oplus_{v\in S}<f_v+g_v,f'_v+g'_v>_v$ and it is non-degenerate and symmetric.

As $\mathcal{F},\mathcal{G}$ are self-dual Selmer structures we see that $C,C_{\mathcal{F}},C_{\mathcal{G}}$ are each their own orthogonal complement under this pairing. This means that $dim_{\mathbb{F}_p}C=dim_{\mathbb{F}_p}C_{\mathcal{F}}=dim_{\mathbb{F}_p}C_{\mathcal{G}}=\frac{1}{2}dim_{\mathbb{F}_p}B$. As

$$C\cong H^1_{\mathcal{F}+\mathcal{G}}(\pi^t(U_s,\eta_s),W)/H^1_{\mathcal{F}\cap\mathcal{G}}(\pi^t(U_s,\eta_s),W) \text{ and}$$
$$C_{\mathcal{F}}\cong H^1_{\mathcal{F}}(\pi^t(U_s,\eta_s),W)/H^1_{\mathcal{F}\cap\mathcal{G}}(\pi^t(U_s,\eta_s),W),$$

we see that

$$dim_{\mathbb{F}_p}H^1_{\mathcal{F}+\mathcal{G}}(\pi^t(U_s,\eta_s),W)/H^1_{\mathcal{F}\cap\mathcal{G}}(\pi^t(U_s,\eta_s),W)=$$
$$\oplus_{v\in S}dim_{\mathbb{F}_p}H^1_{\mathcal{F}}(\pi^t_v(U_s,\eta_s),W)/H^1_{\mathcal{F}\cap\mathcal{G}}(\pi^t_v(U_s,\eta_s),W)$$

Now, we define a pairing

$$[,]:H^1_{\mathcal{F}+\mathcal{G}}(\pi^t(U_s,\eta_s),W)\times H^1_{\mathcal{F}+\mathcal{G}}(\pi^t(U_s,\eta_s),W)\to\mathbb{F}_p$$

by $[x,y]=<x_{\mathcal{F}},y_{\mathcal{F}}>_B$, where $<,>_B$ is the pairing defined above. The pairing $[,]$ is skew-symmetric and the kernel is exactly $H^1_{\mathcal{F}}(\pi^t(U_s,\eta_s),W)+H^1_{\mathcal{G}}(\pi^t(U_s,\eta_s),W)$. Thus, we have a non-degenerate, skew-symmetric pairing on

$$H^1_{\mathcal{F}+\mathcal{G}}(\pi^t(U_s,\eta_s),W)/(H^1_{\mathcal{F}}(\pi^t(U_s,\eta_s),W)+H^1_{\mathcal{G}}(\pi^t(U_s,\eta_s),W))$$

and as p is odd, we see that

$$dim_{\mathbb{F}_p} H^1_{\mathcal{F}+\mathcal{G}}(\pi^t(U_s,\eta_s),W) \equiv H^1_{\mathcal{F}}(\pi^t(U_s,\eta_s),W) + H^1_{\mathcal{G}}(\pi^t(U_s,\eta_s),W) \pmod 2$$

Working modulo 2, we see that

$dim_{\mathbb{F}_p} H^1_{\mathcal{F}}(\pi^t(U_s,\eta_s),W) - dim_{\mathbb{F}_p} H^1_{\mathcal{G}}(\pi^t(U_s,\eta_s),W) \equiv dim_{\mathbb{F}_p} H^1_{\mathcal{F}}(\pi^t(U_s,\eta_s),W) + dim_{\mathbb{F}_p} H^1_{\mathcal{G}}(\pi^t(U_s,\eta_s),W)$

$= dim_{\mathbb{F}_p} H^1_{\mathcal{F}}(\pi^t(U_s,\eta_s),W) + H^1_{\mathcal{G}}(\pi^t(U_s,\eta_s),W) + dim_{\mathbb{F}_p} H^1_{\mathcal{F}\cap\mathcal{G}}(\pi^t(U_s,\eta_s),W)$

$\equiv dim_{\mathbb{F}_p} H^1_{\mathcal{F}+\mathcal{G}}(\pi^t(U_s,\eta_s),W) - dim_{\mathbb{F}_p} H^1_{\mathcal{F}\cap\mathcal{G}}(\pi^t(U_s,\eta_s),W)$

$= \sum_{v\in S} H^1_{\mathcal{F}}(\pi^t_v(U_s,\eta_s),W)/H^1_{\mathcal{F}\cap\mathcal{G}}(\pi^t_v(U_s,\eta_s),W).$

□

3. The second selmer structure

The definition and main results for the second Selmer structure are entirely the same as in [MR] and [MRS], so we merely outline the main ideas and refer the reader to the two papers for the proofs. The two modifications that we will explain later in this section are the self-duality of the second Selmer structure and a variation of Flach's generalisation of the Cassels-Tate pairing.

3.1. **Definition and main properties.** For every cyclic extension L/K of degree p^n contained in F, one can define an abelian variety $A_L = I_L \otimes A$, where I_L is an ideal of the maximal order R_L of $\mathbb{Q}[Gal(L/K)]$. If $\wp$ is the unique prime ideal lying above p in R_L, it turns out that $I_L = \wp^{p^{n-1}}$.

$G = Gal(F/K)$ acts on $Res^F_K(A)$ via its action on A, which factors through R_L. In other words, we have the following sequence

$$\mathbb{Z}[G] \twoheadrightarrow R_L \hookrightarrow End_K(A_L).$$

$A_L \subset Res^F_K(A)$, and there is an isogeny $\oplus_L A_L \cong Res^F_K(A)$. This gives us a G-equivariant decomposition of the p-Selmer group of A, $Sel_p(A/F) \cong \oplus_L Sel_p(A_L/K)$, which we will exploit later. We can think of $A = A_K$ and thus we see that $A[p] = A \cap A_L = A_L[\wp]$ inside $Res^F_K(A)$.

Using the Kummer injection, one can now define the second Selmer structure $H^1_{\mathcal{A}}(\pi_v(U_s,\eta_s),A[p])$ as the image of the composition map

$$A_L(K_v)/\wp A_L(K_v) \hookrightarrow H^1(\pi_v(U_s,\eta_s),A_L[\wp]) \cong H^1(\pi_v(U_s,\eta_s),A[p]).$$

As we are working with primes $q > 2d+1$, the second Selmer structure also factors through the tame fundamental group, and thus $H^1_{\mathcal{A}}(\pi_v(U_s,\eta_s),A[p]) \subset H^1(\pi_v^t(U_s,\eta_s),A[p])$

3.2. **Self-duality.** Since the abelian variety A_L does not have a polarization prime to p (see [H]), there is no Weil pairing so local Tate duality doesn't follow as in the first Selmer structure. Let R_L, A_L be as in the previous section, $G = Gal(L/K)$, $R = R_L \otimes \mathbb{Z}_p$, with G_K acting trivially on R, so that R is the cyclotomic ring over $\mathbb{Z}_p$ generated by p^n-th roots of unity. Let i be the involution of R_L (resp R) induced by $\zeta \to \zeta^{-1}$, for p^n-th roots of unity $\zeta \in R_L$ (resp R).

We first observe that

$$A[p] \cong A_L[\wp] \cong T_p(A_L)/\wp T_p(A_L) \cong T_p(A_L) \otimes \mathbb{Q}_p/\mathbb{Z}_p[\wp].$$

$H^1_{\mathcal{A}}(\pi_v^t(U_s,\eta_s),A[p])$ can also be defined as the image of $A_L(K_v)$ under the composition

$$(1)\ A_L(K_v) \to H^1(\pi_v^t(U_s,\eta_s),T_p(A_L)) \to H^1(\pi_v^t(U_s,\eta_s),T_p(A_L)/\wp T_p(A_L)).$$

Following the same proof as in Lemma 1.3.8 of [R], using $\pi_v^t(U_s,\eta_s)$ instead of the Galois group, we see that the above image of $A_L(K_v)$ is the same as the preimage of $A_L(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ under the mapping

$$(2)\ H^1(\pi_v^t(U_s,\eta_s),T_p(A_L)\otimes\mathbb{Q}_p/\mathbb{Z}_p[\wp]) \to H^1(\pi_v^t(U_s,\eta_s),T_p(A_L)\otimes\mathbb{Q}_p/\mathbb{Z}_p)$$

Hence, to show that $H^1_{\mathcal{A}}(\pi_v^t(U_s,\eta_s),A[p])$ is self-dual we need to first define a pairing on

$$H^1(\pi_v^t(U_s,\eta_s),T_p(A_L)/\wp T_p(A_L)) \times H^1(\pi_v^t(U_s,\eta_s),T_p(A_L)\otimes\mathbb{Q}_p/\mathbb{Z}_p[\wp]),$$

and show that under this pairing the image of (1) and preimage of (2) annihilate each other.

In [MR] a pairing is defined on $T_p(A_L)\times T_p(A_L) \to R\otimes_{\mathbb{Z}_p}\mathbb{Z}_p(1)$ as follows:

As $T_p(A_L) = I_L \otimes T_p(A)$, we define $< \alpha \otimes x, \beta \otimes y >_R = (\pi^{-2p^{n-1}\alpha\beta^i}) \otimes e(x, y)$, where e denotes the Weil pairing.

This pairing is perfect, G_K-equivariant and i-adjoint which leads to a perfect, i-adjoint cup-product pairing on

$$H^1(\pi_v^t(U_s, \eta_s), T_p(A_L)) \times H^1(\pi_v^t(U_s, \eta_s), T_p(A_L) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \to \mathbb{Q}_p/\mathbb{Z}_p,$$

under which the images of $A_L(K_v)$ and $A_L(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ are orthogal complements of each other. This induces a pairing λ on:

$$H^1(\pi_v^t(U_s, \eta_s), T_p(A_L)/\wp T_p(A_L)) \times H^1(\pi_v^t(U_s, \eta_s), T_p(A_L) \otimes \mathbb{Q}_p/\mathbb{Z}_p[\wp]) \to \mathbb{F}_p.$$

Now that we have the required pairing, we need to show the orthogonal relation.

Let $T = T_p(A_L)$, $V = T \otimes \mathbb{Q}_p$, $W = V/T = T \otimes \mathbb{Q}_p/\mathbb{Z}_p$, and $W_{p^n} = A_L[p^n] = T/p^nT \subset W$. Let $H^1_f(\pi_v^t(U_s, \eta_s), V) = H^1(G_v/I_v, V)$, and we define $H^1_f(\pi_v^t(U_s, \eta_s), T)$ and $H^1_f(\pi_v^t(U_s, \eta_s), W)$ as the images and preimages of $H^1_f(\pi_v^t(U_s, \eta_s), V)$ under the maps

$$H^1_f(\pi_v^t(U_s, \eta_s), T) \to H^1_f(\pi_v^t(U_s, \eta_s), V) \to H^1_f(\pi_v^t(U_s, \eta_s), W)$$

and $H^1_f(\pi_v^t(U_s, \eta_s), W_p)$ to be the inverse image of $H^1_f(\pi_v^t(U_s, \eta_s), W)$ under the natural map

$$H^1(\pi_v^t(U_s, \eta_s), W_p) \to H^1(\pi_v^t(U_s, \eta_s), W).$$

By Lemma 1.4.3 of [R], $H^1_f(\pi_v^t(U_s, \eta_s), W_\wp)$ is orthogonal to $H^1_f(\pi_v^t(U_s, \eta_s), W_\wp)$ and since

$$W_\wp \cong T_p(A_L)/\wp T_p(A_L) \cong T_p(A_L) \otimes \mathbb{Q}_p/\mathbb{Z}_p[\wp] = A_L[\wp] = A[p],$$

the second Selmer structure $H^1_{\mathcal{A}}(\pi_v^t(U_s, \eta_s), A[p])$ is self-dual.

3.3. **Flach's pairing.** To make use of parity arguments in this paper, it is necessary that $dim_{\mathbb{F}_p} Ш/Ш_{div}[\wp]$ is even, where $Ш_{div}$ is the maximal divisible subgroup. In the case of an elliptic curve E it is known due to the Cassels-Tate pairing, but for abelian varieties it was generalised (in fact for motives) by Flach.

We will modify Flach's pairing (see [F]) and construct a perfect, $Gal(K/k)$-equivariant, skew-Hermitian pairing, on $Ш_{/div} := Ш/Ш_{div}$. The key modification is to work with the tame fundamental group instead of the full Galois group, so we give a sketch of the pairing here.

Let T, V, W be as in the previous section. Consider the short exact sequence

$$0 \longrightarrow T \xrightarrow{i} V \xrightarrow{p} W \longrightarrow 0.$$

If G is a topological group, then p has a continuous splitting and as W has the discrete topology, we see that $0 \to C^*(G,T) \to C^*(G,V) \to C^*(G,W) \to 0$ ([R])

Now, we replace G with $\pi^t(U_s,\eta_s)$, and let B_v be a subspace of $H^1(\pi_v^t(U_s,\eta_s),V)$. We define B as

$$0 \to B \to H^1(\pi^t(U,\eta),V) \to \prod_v H^1(\pi_v^t(U,\eta),V)/B_v \to 0$$

The p-Selmer group as

$$0 \to Sel_p(A_L/K) \to H^1(\pi^t(U,\eta),W) \to \prod_v H^1(\pi_v^t(U,\eta),W)/p_*(B_v) \to 0$$

and $Ш(A_L/K)$ as

$$\begin{aligned}0 \to Ш(A_L/K) \to H^1(\pi^t(U_s,\eta_s),W)/p_*(B) \to \\ \prod_v H^1(\pi_v^t(U,\eta),V)/p_*(B_v) \to 0\end{aligned}$$

To define a pairing on $Ш(A/K)$, we first define a pairing on $Sel_p(A/K)$.

Let $a,a' \in Sel_p(A_L/K)$. By the splitting above we have the following commutative diagram:

$$\begin{array}{ccccc} & & C^1(\pi^t(U_s,\eta_s),V) & \longrightarrow & C^1(\pi^t(U_s,\eta_s),W) \\ & & \downarrow d & & \downarrow d \\ C^2(\pi^t(U_s,\eta_s),T) & \longrightarrow & C^2(\pi^t(U_s,\eta_s),V) & \longrightarrow & C^2(\pi^t(U_s,\eta_s),W) \end{array}$$

We can lift a,a' to $\alpha,\alpha' \in Z^1(\pi^t(U_s,\eta_s),W)$, and by the diagram above to $\beta,\beta' \in C^1(\pi^t(U_s,\eta_s),V)$ and therefore $d\beta, d\beta' \in C^2(\pi^t(U_s,\eta_s),V)$.

Using the cup-product pairing we see that $d\beta \cup \beta' \in Z^3(\pi^t(U_s,\eta_s),V)$, but $H^3(\pi^t(U_s,\eta_s),V) = 0$. Hence, $d\beta \cup \beta' = d\epsilon$, where $\epsilon \in C^2(\pi^t(U_s,\eta_s),\mathbb{Q}/\mathbb{Z}(1))$.

Given $\alpha' \in Sel_p(A_L/K)$, by definition $res_v(\alpha') \in p_*(B_v) \Rightarrow res_v(\alpha') = \beta'_v \in Z^1(\pi^t(U_s,\eta_s),V)$. Define $c_v = res_v(\beta) \cup \beta'_v - res_v(\epsilon)$. We see that $c_v \in C^2(\pi^t_v(U_s,\eta_s),\mathbb{Q}/\mathbb{Z}(1))$.

Finally, we define the pairing $< a, a' >:= \sum_v inv_v(c_v)$. We know that this is a finite sum as $H^2(\pi^t_v(U_s,\eta_s),\mathbb{Q}/\mathbb{Z}(1)) = 0$ for almost all primes v.

Now that we have this pairing, the result about it being non-degenerate, Galois equivariant and skew-symmetric follows exactly as in Theorem 1 and 2 of [F]. To finish the argument we use Thm A.12 of [MR] and as we have a non-degenerate, skew-symmetric, Galois equivariant pairing on $\text{Ш}_{/div}[\wp]$ we see that it has even $\mathbb{F}_p$-dimension.

4. Local invariants

Using the two Selmer structures $\mathcal{A}, \mathcal{E}$, we can now define the local constants and then calculate them.

Definition. For every prime v of K, define $\delta_v \in \mathbb{Z}/2\mathbb{Z}$ by

$$\delta_v := dim_{\mathbb{F}_p}(H^1_{\mathcal{E}}(\pi_v(U,\eta), A[p])/H^1_{\mathcal{E}\cap\mathcal{A}}(\pi_v(U,\eta), A[p]))(mod 2)$$

Let c be an automorphism of order 2 of K, $k \subset K$ be the fixed field of c, and suppose that A is defined over k. Fix a cyclic extension L/K of degree p^n, such that L is Galois over k with dihedral Galois group.

One of the key lemmas in computing the local invariants δ_v is the following (see Prop 5.2 of [MR]).

Lemma 4.1. $H^1_{\mathcal{A}\cap\mathcal{E}}(\pi^t_v(U,\eta), A[p]) \cong A(K_v) \cap N_{L/M}(A(L_v))$.

Proof. If $x \in A(K_v)$, then its image in $H^1_{\mathcal{E}}(\pi^t_v(U,\eta), A[p])$ is given by $\gamma \mapsto y^{\gamma\otimes 1} - y$, where $y \in A(\overline{K}_v)$ and $py = x$. Similarly, if $x \in A_L(K_v)$, then its image in $H^1_{\mathcal{A}}(\pi^t_v(U,\eta), A[p])$ is given by $\gamma \mapsto \beta^{\gamma\otimes 1} - \beta$, where $\beta \in A_L(\overline{K}_v)$ and $\pi\beta = x$ (π is a generator of $\wp$). So $x \in H^1_{\mathcal{E}\cap\mathcal{A}}(\pi^t_v(U,\eta), A[p]) \Leftrightarrow \exists \beta \in A_L(\overline{K}_v) : \pi\beta \in A_L(K_v), \beta^{\gamma\otimes 1} - \beta = y^{\gamma\otimes 1} - y$, $\forall \gamma \in \pi^t_v(U,\eta)$.

Notice that $\widehat{\pi} = (1 \otimes \sigma) - 1$ restricts to 0 on $A(\overline{K}_v)$. So, $\widehat{\pi}(\beta^{\gamma\otimes 1} - \beta) = \widehat{\pi}(y^{\gamma\otimes 1} - y) = 0$, which means that $\widehat{\pi}\beta^{\gamma\otimes 1} = \widehat{\pi}\beta$, $\forall \gamma \in \pi_v^t(U,\eta) = Gal(K_v^{tr}/K_v)$. So $\pi\beta \in A_L(K_v)$ ($\widehat{\pi} = \pi$ in $A_L(K_v)$).

By Thm 5.8(ii) of [MRS], we see that $A_L(\overline{K}_v) = \{x \in A(\overline{K}_v \otimes L) : \sum_{g\in G(L/K)} 1 \otimes g(x) = 0\}$. Thus, $\beta \in A_L(\overline{K}_v) \Leftrightarrow \beta \in A(\overline{K}_v \otimes L)$ such that $N_{L/M}(\beta) = 0$. We also see that $\beta^{\gamma\otimes 1} - \beta = y^{\gamma\otimes 1} - y$, $\forall \gamma \in \pi_v^t(U,\eta) \Leftrightarrow y - \beta = (y-\beta)^{\gamma\otimes 1}$, $\forall\gamma \Leftrightarrow y - \beta \in A(K_v \otimes L) = A(L_v)$.

We can think of $A(\overline{K_v})$ as $A(\overline{K_v} \otimes L)^G$. As $y \in A(\overline{K_v})$, then $N_{L/M}(y) = py = x$. Hence, $H^1_{\mathcal{A}\cap\mathcal{E}}(\pi_v^t(U,\eta), A[p]) \cong A(K_v) \cap N_{L/M}(A(L_v))$.

□

Proposition 4.2. *$\delta_v = 0$ for a prime v where A has good reduction, and $v^c = v$.*

Proof. Since we are working with a function field of characteristic q different from p, by Thm 5.6 of [MR], we see that $\delta_v \equiv dim_{\mathbb{F}_p} A(K_v)[p] \mod 2$. The proof is exactly the same.

To show that $\delta_v = 0$, we need to prove that $dim_{\mathbb{F}_p} A(K_v)[p]$ is even. We follow the proofs of Lemmas 6.5 and 6.6 of [MR] modifying them since we are working with the tame fundamental group.

If v is a prime in K, let w be the prime of L above v and u the prime of k below v. Let I be the inertia subgroup of $Gal(L_w/k_u)$. By assumption v is fixed by c and $Gal(L/k)$ is dihedral, so $Gal(L_v/k_u)$ is also dihedral. Thus, the only subgroups of $Gal(L_v/k_u)$ with cyclic quotient are $Gal(L_v/k_u)$ or $Gal(L_v/K_v)$ which means that I is one of them, and so L_w/K_v is totally ramified.

If v was ramified in K/k, then I would be dihedral of order $2[L_w : K_v]$. If l is the residue characterstic of K_v, then the maximal abelian quotient of I has order 2, so $[L_w : K_v]$ is a power of l, which means $l = p$. Thus, v is unramified in K/k.

Let ϕ be the Frobenius generator of $Gal(K_v^{ur}/k_u)$ and ϕ^2 the generator of $Gal(K_v^{ur}/K_v)$. By assumption, L is Galois over k with dihedral Galois group so c acts by inversion on $Gal(L_w/K_v)$, which is cyclic of degree p^n, so ϕ acts by inversion on $\mu_p \subset \kappa^*$, where κ is the residue field of K.

As $A(K_v)[p] = A[p]^{\phi^2=1}$ and $A[p]$ has even dimension over $\mathbb{F}_p$, we will show that ϕ^2 is either 0 or the identity.

Let α, β be the eigenvalues of ϕ acting on $A[p]$, then by the Weil pairing e on $A[p] \times A[p]$, we know that $e(\alpha x, \beta y) = e(x^\phi, y^\phi) = e(x, y)^\phi$, but as ϕ acts by inversion on μ_p, we see that $\alpha\beta = -1$.

If $\{\alpha, \beta\} = \{1, -1\}$, the action of ϕ is diagonalisable so ϕ^2 is the identity. If $\alpha \neq \pm 1$, then 1 is not an eigenvalue of ϕ^2 acting on $A[p]$, so $\phi^2 = 0$.

Thus, $\delta_v = dim_{\mathbb{F}_p} A(K_v)[p]$ is even for primes $v \in K$ of good reduction, which ramify in L/K.

$\square$

5. Main results

Proposition 5.1. *$corank_{\mathbb{Z}_p} Sel_p(A/K) - corank_{R_p} Sel_p(A_L/K) \equiv \sum_{v\in S} \delta_v (\mod 2)$, where $R_p = R \otimes \mathbb{Z}_p$.*

Proof. By Thm 2.2 we know that

$$dim_{\mathbb{F}_p} H^1_{\mathcal{F}}(\pi^t(U_s, \eta_s), W) - dim_{\mathbb{F}_p} H^1_{\mathcal{G}}(\pi^t(U_s, \eta_s), W) \equiv \sum_{v\in S} dim_{\mathbb{F}_p}(H^1_{\mathcal{F}}(\pi^t_v(U_s, \eta_s), W)/H^1_{\mathcal{F}\cap\mathcal{G}}(\pi^t_v(U_s, \eta_s), W)) (\mod 2).$$

By Prop 2.1 of [MR], we see that for a self dual Selmer structure $\mathcal{E}$,

$$corank_{\mathbb{Z}_p} Sel_{p^\infty}(A/K) \equiv dim_{\mathbb{F}_p} H^1_{\mathcal{E}}(\pi(U_s, \eta_s), A[p]) - dim_{\mathbb{F}_p} A(K_v)[p] (\mod 2).$$

Using a proof similar to Prop 2.1 of [MR], we get

$$corank_{R_p} Sel_{p^\infty}(A_L/K) \equiv dim_{\mathbb{F}_p} H^1_{\mathcal{A}}(\pi(U_s, \eta_s), A[p]) - dim_{\mathbb{F}_p} A(K_v)[p] (\mod 2).$$

Note that in this statement, it is essential that $dim_{\mathbb{F}_p}Ш_{/div}(A_L)$ is even (section 3). Using these three relations, we see that $corank_{\mathbb{Z}_p}Sel_p(A/K) - corank_{R_p}Sel_p(A_L/K) \equiv \sum_{v\in S}\delta_v(\mod 2)$.

□

We are now in a position to state and prove the main result of the paper.

Theorem 5.2. *Let K/k be a quadratic extension of function fields, char $k = q$, with non-trivial automorphism c, A an abelian variety over k and F an abelian p-extension of K, dihedral over k (i.e. F is Galois over k and c acts by inversion on $Gal(F/K)$). If*

- *A has good reduction at primes v of K, which ramify in in F/K and are fixed by c*
- *$corank_{\mathbb{Z}_p}Sel_p(A/K)$ is odd*

then $corank_{R_p}Sel_p(A/F) \geq [F : K]$.

Proof. By Sec 3.1 we know that

$$Sel_p(A/F) \cong \oplus_L Sel_p(A_L/K)$$

where L runs through the cyclic extensions of K in F.

Let S be the set of primes v in K that ramify in F, $v^c = v$ and where A has good reduction. Then, by Prop 5.1

$$corank_{\mathbb{Z}_p}Sel_p(A/K) - corank_{R_p}Sel_p(A_L/K) \equiv \sum_{v\in S}\delta_v(\mod 2).$$

By Prop 4.2, we know that $\delta_v = 0$ for primes $v \in S$, hence

$$corank_{\mathbb{Z}_p}Sel_p(A/K) \equiv corank_{R_p}Sel_p(A_L/K)(\mod 2).$$

We assumed that $corank_{\mathbb{Z}_p}Sel_p(A/K)$ is odd, hence $corank_{\mathbb{Z}_p}Sel_p(A_L/K)$ is at least one. Thus, $corank_{\mathbb{Z}_p}Sel_p(A/F) \geq [F : K]$.

□

6. Concluding Remarks

1) Since we assume that $\mathbb{Z}_p$-corank of $Sel_p(A/K)$ is odd it would be interesting to know when it can be forced to be odd. It is not clear if the methods of [MR] would work here.

2) In [MR1] the main results of [MR] have been extended for non-abelian extensions of number fields. Their results should extend to this paper as well.

3) As we are not familiar with flat cohomology we have avoided the equal characteristic case. We hope to resolve this case in future work.

4) The methods of [MR] have also been used by the same authors to study Hilbert's tenth problem in [MR2]

7. Acknowledgements

The author was supported by a CNPq post-doctoral fellowship hosted by Amilcar Pacheco. The author would like to thank him for suggesting the problem and for his help over the last two years.

References

[DD1] T. Dokchitser and V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares* Ann. of Math. (2) 172 (2010), no. 1, 567-596

[DD2] T. Dokchitser and V. Dokchitser, *Regulator constants and the parity conjecture* Invent. Math. 178 (2009), no. 1, 23-71.

[E] J. Ellenberg, *Selmer groups and Mordell-Weil groups* Compos. Math. 142, 1215-1230 (2006)

[F] M. Flach, *A generalisation of the Cassels-Tate pairing* J. Reine Angew. Math. 412 (1990), 113-127.

[H] E. Howe, *Isogeny classes of abelian varieties with no principal polarizations* Moduli of Abelian Varieties (Texel Island, 1999), Progr. Math. 195, Birkhauser, Basel (2001), 203-216.

[M] J. Milne, *Etale cohomology* Princeton University Press, Princeton (1980).

[MR] B. Mazur and K. Rubin *Finding large Selmer rank via an arithmetic theory of local constants* Ann. of Math. (2) 166 (2007), no. 2, 579-612.

[MR1] B. Mazur and K. Rubin, *Growth of Selmer rank in nonabelian extensions of number fields* Duke Math. J. 143 (2008), no. 3, 437-461.

[MR2] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem* Invent. Math. 181 (2010), no. 3, 541-575.

[MRS] B. Mazur, K. Rubin and A. Silverberg *Twisting commutative algebraic groups* J. Algebra 314 (2007), 419-438.

[P] A. Pacheco, *Selmer groups of abelian varieties in extensions of function fields* Math. Z. 261 (2009), no. 4, 787-804.

[R] K. Rubin *Euler Systems* Ann. of Math. Studies 147, Princeton Univ. Press, Princeton (2000).

Aftab Pande

email: aftab.pande@gmail.com

Instituto de Matematica

Universidade Federal do Rio de Janeiro

Rio de Janeiro, Brasil